Research Paper COMPUTER SCIENCE

Secure Routing Protocols in Wireless AD-HOC Networks – A Survey

Dr. Banta Singh Jangra | Asstt. Professor, Deptt. Of Computer Science, FGM Govt. PG College, Adampur (Hisar) Haryana, India

Manish Kumar Naga | Research Scholar, Ph.D.-Computer Science, Deptt. Of Computer Science, Jyoti Vidyapeeth Women University, Jaipur (Rajasthan) India

ABSTRACT

In this paper we are concerned with security of routing protocols in ad hoc wireless networks. Routing is an important operation, providing the communication protocol for data delivery between wireless devices. Assuring a secure routing protocol is a challenging task since ad hoc wireless networks are highly vulnerable to security attacks due to their unique characteristics. Traditional routing protocols designs do not address security, and are based on a mutual trust relationship between nodes. The wireless nature of communication and lack of any security infrastructure raises several security problems. We examined and classified major routing attacks and present a comprehensive survey on the state-of-the-art mechanisms and solutions designed to defeat such attacks. The current security mechanisms, each defeats one or few routing attacks. Designing routing protocols resistant to multiple attacks remains a challenging task.

KEYWORDS Routing Protocols, Ad-hoc Networks, MAC

1. Introduction

On wireless computer networks, ad hoc is a method for wireless devices to directly communicate with each other. Operating in ad-hoc mode allows all wireless devices within range of each other to discover and communicate in peer-to peer way without linking central access. An ad-hoc network tends to feature a small group of devices all in very close proximity to each other. Performance suffers as the number of devices grows, and a large ad-hoc network quickly becomes difficult to manage communication for mobile hosts. Wireless networks provide fast access to information and com-Putting, eliminating the barriers of distance, time, and location for many applications rang from joint, distributed mobile computing to disaster recovery (such as fire, flood, earthquake), law enforcement (crowd control, search and rescue) and military communications . An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any well-known infrastructure or centralized administration.

In this paper we are anxious with security of routing protocols in ad hoc wireless networks. Routing is a significant operation, providing the statement protocol for data release between wireless devices. Assuring a secure routing protocol is a challenging task since ad hoc wireless networks are highly vulnerable to security attacks due to their unique characteristics. Conventional routing protocols designs do not address safety, and are based on a mutual trust relationship between nodes. The wireless nature of message and lack of any security infrastructure raises several security problems. There are two different types of wireless networks.



Figure 1: Ad hoc Security

2. Indication of Routing Protocols in Ad-Hoc Wireless Networks

Routing is an imperative process, those data exchanging flanked by wireless devices. Each wireless node acts as a router in the routing protocol. Routing relies therefore on an implied trust relationship among participating devices. Main routing responsibilities are exchanging the routing information, decision a practicable path between starting place and purpose based on various metrics, and path maintenance. The major requirements of a routing protocol are

(1) Minimum route achievement delay.
(2) Quick route reconfiguration in the case of path breaks.
(3) loop-free routing.
(4) Distributed routing protocol.
(5) Low control over- head.
(6) Scalability with network size.
(7) Security support as demanded by the application.
(8) Support of time-sensitive traffic, and
(9) Security and privacy.

2.1 Hybrid Routing Protocols

A number of ad hoc network routing protocols are hybrid of practical and immediate mechanisms. Examples of hybrid routing protocols are Zone Routing Protocol (ZRP) , Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) , etc. ZRP is a hybrid of proactive and reactive routing protocols. The network is divided in zones, where every zone is an r-hop neighborhood of a join. The intra-zone routing protocol is a proactive routing protocol, while the inter-zone routing protocol is a reactive routing protocol. By varying, we can control the routing update control traffic. Distribution in Ad Hoc Wireless Networks Broadcasting refers to the function of sending a message to all other hosts in the network. Broadcasting is used for the route discovery in reactive routing protocols. In a portable environment, distribution is expected to be used more regularly because nodes mobility might trigger path disconnecting and thus route discovery is invoked as part of the path maintenance procedure.

2.2 Reactive Routing Protocols

In the reactive routing protocols, a route detection method is initiated only when a node does not know a path to a ob-

jective it wants to converse with. In the case of movable ad hoc network, reactive routing protocols have been established to carry out improved with considerably lower overheads than proactive routing protocols as they are capable to respond rapidly to the many changes that may take place in node connectivity, and yet are able to decrease (or do away with) direction-finding overhead in periods or areas of the network in which changes are less frequent. A reactive routing protocol has two main operations, route discovery (usually broadcasting using a form of controlled flooding) and route maintenance. Various reactive protocols have been proposed in literature such as Ad Hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) , Temporally Ordered Routing Algorithm (TORA) , etc. DSR is a source routing protocol, and thus has the property that each data packet carries the source-destination path in its header.

2.3 Proactive Routing Protocols

In proactive routing protocols, nodes exchange routing information periodically in order to maintain consistent and accurate routing information. When a node has to transmit data to a destination, the path can be computed rapidly based on the updated information available in the routing table. The disadvantage of using a proactive protocol is high overhead needed to maintain up to date routing information. In ad hoc wireless networks, node mobility triggers a dynamic topology that might require a large number of routing updates. This has a negative impact on resource constrained wireless devices, bandwidth utilization, and throughput. The protocols in this category are typically extensions of the wired net- work routing protocols. Examples include Destination Sequence Distance Vector (DSDV), Wireless Routing Protocol (WRP), Optimized Links State Routing (OLSR), etc.

3 General ideas of selected Protocols

There are uni casts, single channel protocols, which are uniform or non-uniform. Uniform protocols are divided to topology-based protocols, in where nodes are aware of the topology information of all other nodes in the network or to destination-based protocols, in where nodes only know the preferred next hop to a destination. One protocol to belong to that topology-based class is GSR (Global State Routing) and the other is DSR (Destination Source Routing). One main difference between these protocols is the scheduling method. GSR is a proactive protocol, which will all the time have the information needed for routing. DSR is on its behalf a reactive protocol, which will obtain needed information only on demand. To destination-based protocols belong such protocols as DSDV, AODV, TORA, ABR and WRP. The well known difference between e.g. DSDV and AODV is the scheduling method. The DSDV is proactive as is WRP, but AODV, TORA and ABR all are reactive protocols. To be classified to single channel, non-uniform protocols there are such protocols as ZRP, FSR, OLSR, CEDAR and CBRP. Form these protocols ZRP, FSR, and OLSR belong to neighbor selection protocols, which have a common feature to select network subsets by individual nodes themselves. In partitioning protocols there are some kind of clustering and cluster head selection mechanism. To partitioning protocols belongs e.g. CEDAR and CBRP.

4. Security Mechanisms and Solutions for Routing Protocols in Ad Hoc Wireless Networks

In ad hoc wireless networks, the secrecy of the key does not ensure the integrity of the message. For this purpose, Message Authentication Code (MAC) is used. It is a hashed representation of a message and even if MAC is known, it is impractical to compute the message that generated it. A MAC, which is a cryptographic checksum, is computed by the message initiator as a function of the secret key and the message being transmitted and it is appended to the message. Next, we present security mechanisms specifically customized for specific routing mechanisms.

4.1 Secure Efficient Ad hoc Distance Vector (SEAD)

Secure Efficient Ad hoc Distance Vector (SEAD) is a proactive routing protocol, based on the design of DSDV. Besides the fields common with DSDV, such as destination, metric, next hop and sequence number, SEAD routing tables maintain a hash value for each entry, as described below.

This paper is concerned with protecting routing updates, both periodic and triggered, by preventing an attacker to forge better metrics or sequence numbers in such update packets. SEAD provides a robust protocol against attackers trying to create in- correct routing state in other node by modifying the sequence number or the routing metric. SEAD does not provide a way to prevent an attacker from tampering next hop or destination field in a routing update. Also, it cannot prevent an attacker to use the same metric and sequence number learned from some recent update message, for sending a new routing update to a different destination.

4.2 ARIADNE

ARIADNE an efficient on-demand secure routing protocol provides security against arbitrary active attackers and relies only on efficient symmetric cryptography. It prevents attackers from tampering uncompromised routes consisting of uncompromised nodes. ARIADNE ensures point-to-point authentication of a routing message by combining a shared key between the two parties and MAC. However, for secure authentication of a routing message, it relies on the TESLA broadcast authentication protocol.

4.3 Secure Routing Protocol (SRP)

Secure Routing Protocol (SRP) , is another protocol extension that can be applied to many of the on demand routing protocols used today. SRP defends against attacks that disrupt the route discovery process and guarantees to identify the correct topological information. The basic idea of SRP is to set up a security association (SA) between a source and a destination node without the need of cryptographic validation of the communication data by the intermediate nodes. SRP suffers from the lack of validation mechanism for route maintenance messages as it does not stop a malicious node from harming routes to which that node already belongs to. SRP is immune to IP spoofing because it secures the binding of the MAC and IP address of the nodes but it is prone to wormhole attacks and invisible node attacks.

4.4 Secure Routing Protocol for Ad Hoc Networks (ARAN)

A Secure Routing Protocol for Ad Hoc Networks (ARAN) is an on demand protocol designed to provide secure communications in managed open environments. Nodes in a managed-open environment exchange initialization parameters before the start of communication. Session keys are exchanged or distributed through a trusted third party like a certification.

4.5 Security Aware Routing (SAR)

Security Aware Routing (SAR) is an on demand routing protocol based on AODV. It integrates the trust level of a node and the security attributes of a route to provide an integrated security metric for the requested route. By incorporating a Quality of Protection (QoP) as a routing metric, the route discovery can return quantifiable secure routes. The QoP vector used is a combination of security level and available cryptographic techniques SAR introduces the notion of a trust hierarchy, where nodes of the ad hoc wireless network are divided into different trust levels such that an initiator can impose a minimum trust level for all the nodes participating in the source-destination communication. Note that a path with the required trust level might not exist even if the network is connected.

5. Security Services and Challenges in Ad-Hoc Wireless Networks

In order to guarantee a dependable information transport over the communication networks and to guard the system resources, a number of security services are mandatory. Based on their objectives, the protection services are confidential in five categories: availability, confidentiality, authentication, integrity and non repudiation.

Services	Techniques
Authenticity	Password, certificate
Authorization	Credential
Integrity	Digest, Digital Signature
Confidentially	Encryption
Non-repudiation	Chaining of digital signature

Table1: Secure Ad hoc Routing Services

(a) Availability: Availability implies that the requested services (e.g. bandwidth and connectivity) are obtainable in a opportune approach while there is a possible problem in the system. Accessibility of a network can be temper for instance by reducing off packets by resource reduction attacks.

(b) Confidentiality: Confidentiality ensures that private in order in the multifaceted is never disclosed to illegal entities. Confidentiality can be achieved by using different encryption techniques so that only the lawful communicating nodes can examine and recognize the transmission. The content discovery attack and position disclosure attack reveals the contents of the message being transmit and bodily in order about a exacting node in that order.

(c) Authenticity: Authenticity is a network examines to agree on a user's uniqueness. Without verification, an attacker can imitate any node, and in this way, one by one node, it can gain organize above the complete system.

(d) Integrity: Integrity guarantees that in order passed on flanked by nodes has not been tempered in the broadcast. Information can be altered both deliberately and unintentionally (for example through hardware glitches, or in case of ad hoc wireless connections through interference).

(e) Non-repudiation: Non-repudiation ensures that the information inventor cannot refute having sent the information. This service is practical for uncovering and separation of compromised nodes in the network. Many verification and secure routing algorithms implemented in ad hoc networks rely on trust-based concepts. The fact that a message can be credited to a exact node helps making these algorithms more protected.

Manipulative a protected ad hoc wireless networks communiqué is a demanding mission due to

(1) Timid wireless communication links,
(2) Nonappearance of a fixed infrastructure,
(3) Reserve constraints (e.g. battery power, bandwidth, memory, CPU processing capacity), and (4) Node mobility that triggers a self-motivated system topology.

The majority of conservative routing protocols intend fails to make obtainable security.

The main necessities of a secure direction-finding procedure are:

(1) Discovery of malicious nodes; such nodes be supposed to be avoided in the routing process,
(2) Declaration of correct route discovery,
(3) Confidentiality of net- work topology; if an attacker learns the network topology, he can attack the bottleneck nodes, detected by studying the traffic patterns. This will result in disturbing the routing process and DoS, and
(4) Firmness next to attacks; the direction-finding procedure must be able to recommence the normal process within a restricted quantity of time after an attack.

6. Security Attacks on Routing Protocols in Ad Hoc Wireless Networks

As long as a secure system can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on ad hoc wireless networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not.

Passive Attack: In passive attacks, an intruder snoops the data ex- changed without altering it. The attacker does not aggressively initiate malicious actions to cheat other hosts. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect. Powerful encryption mechanism can alleviate these attackers by making difficult to read overheard packets.

Active Attack: In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks: External Attacks are carried by nodes that are not legitimate part of the network. Such attacks can be defended by using encryption, firewalls and source authentication. To perform an active attack the attacker must be able to inject arbitrary packets into the network.

Black Hole

A malicious node uses the routing protocol to advertise itself as having the shortest path to nodes whose packets it wants to intercept. In a flooding based protocol such as AODV, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised. If the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to perform a denial-of-service attack, or alternatively use its place on the route as the first step in a man-in-the-middle attack.

REFERENCES

[1] J. Barkley, NIST Special Publication: Symmetric Key Cryptography, http://csrc.nist.gov/publications/nistpubs/800-7/node208. html | [2] S. Buchegger and J. L. Boudec, Performance Analysis of the CONFI- DANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks, In Proc. of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Jun. 2002 | [4] D. Coppersmith and M. Jakobsson, Almost Optimal Hash Sequence Traversal, In Proc. of The Sixth Intl. Conf. on Financial Cryptography(FC 2002), Lecture Notes in Computer Science, Springer 2002. | [5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks, ACM CCS 2003, Oct.2003, pp. 42-51. | [6] Z. J. Haas, The Routing Algorithm for the Reconfigurable Wireless Net-works, Proc. of ICUPC 1997, Vol 2, Oct. 1997, pp. 562-566. | [8] Y. -C. Hu, D. B. Johnson, and A. Perrig, Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, Mobicom'02, 2002. | [9] Y. -C. Hu, D. B. Johnson, and A. Perrig, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, WiSe 2003, 2003. | [10] Y. -C. Hu, D. B. Johnson, and A. Perrig, Efficient Security Mechanisms for Routing Protocols, The 10th Annual Network and Distributed System Security Symp. (NDSS), Feb. 2003. | [11] Y. -C. Hu, A. Perrig, and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Infocom 2003. | [13] R. Kravets, S. Yi, and P. Naldurg, A Security-Aware Routing Proto-col for Wireless Ad Hoc Networks, In ACM Symp. on Mobile Ad Hoc Networking and Computing, 2001. | [14] S. Murthy and J. J. Garcia-Luna-Aceves, An Efficient Routing Protocol for Wireless Networks, ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, Vol 1, No2, Oct. 1996, pp. 183-197. | [15] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Archi-tectures and Protocols, Prentice Hall PTR, 2004. | [16] J. Newsome, E. Shi, D. Song, and A. Perrig, The Sybil Attack in SensorNetworks: Analysis & Defenses, Proc. of the 3rd Intl. Symp. on Infor-mation Processing in Sensor Networks, 2004. | [17] P. Papadimitratos and Z. J. Haas, Secure Routing for Mobile Ad hocNetworks, In Proc. of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), Jan. 2002. | [18] V. D. Park and M. S. Corson, A Highly Adaptive Distributed Routing Algorithm for MobileWireless Networks, IEEE Infocom 1997, Apr. 1997,pp. 1405-1413. | [19] C. E. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, SIGCOMM'94 Conf. on Communications Architectures, Protocols and Applications, Aug. 1994, pp. 234-244. | [20] C. E. Perkins and E. M. Royer, Ad Hoc On-Demand Distance Vector Routing, IEEE Workshop on Mobile Computing Systems and Applica-tions 1999, Feb. 1999, pp. 90-100. |